

CHAPTER 14

TABLE OF CONTENTS

Section A - Medical Information Systems (MIS) Plan.....	1
1. Purpose.....	1
2. Background.....	1
3. Coast Guard Policy on Privacy and Security.....	2
4. Applicability and Scope.....	4
5. Objectives.....	4
6. Definitions.....	5
7. Organizational Responsibilities.....	5
Section B - Medical Information System.....	7
1. Background.....	7
2. Systems.....	7
Section C - Medical Readiness System (MRS).....	15
1. MRS Implementation	15
2. MRS Medical Readiness Parameters.....	15
3. MRS Record Waiver Information	15
4. Question on MRS	15
5. Access Instructions.....	15

CHAPTER 14. MEDICAL INFORMATION SYSTEMS (MIS) PROGRAM

Section A - Medical Information Systems (MIS) Plan.

1. Purpose.

- a. The Medical Information System (MIS) program described here follows the policy established by the Office of Health Services, outlines systems and assigns responsibility for the administration of the MIS. The MIS is a key component for the overall management of Coast Guard clinics and sickbays. MIS is a dynamic tool, which will provide a comprehensive electronic solution for tracking operational medical readiness, health systems management, and patient access to care. The Health and Safety Directorate, Maintenance and Logistics Commands, unit Commanding Officers, and health care providers are responsible for ensuring successful implementation of the Coast Guard Medical Information Systems.

2. Background.

- a. There is an ongoing need for Commandant, Area Commanders, and field level Commanding Officers to assess medical operational readiness. Additionally, the Coast Guard Health Services program needs to accurately capture workload, performance, and productivity through standardized methodology. Proper analysis of health care data provides the ability to realign assets where they are most needed to deliver timely quality health care. The full implementation of the Composite Health Care System I/II (CHCS), Shipboard Automated Medical System (SAMS), Dental Common Access System (DENCAS), and Third Party Collections Program (TPC) will significantly enhance our ability to provide this information as needed.
- b. Federal statutes impose strict requirements for managing government information. The most pertinent Federal statutes that govern information include:
 - (1) Federal Records Act (Public Law 81-754): Sets policy for and mandates establishment of agency programs for the management of Federal records.
 - (2) Freedom of Information Act (Public Law 90-23): Provides policy to ensure public access to Federal government information.
 - (3) Paperwork Reduction Act (Public Law 96-511): Recognizes information as a Federal resource and directs agencies to establish specific programs for management of the resource and associated elements.
 - (4) Paperwork Reduction Reauthorization Act (Public Law 99-500): Defines information resources management and directs further program management requirements.

- (5) Privacy Act (Public Law 93-579): Provides policy and safeguards to protect privacy of individuals.
 - (6) Health Insurance Portability and Accountability Act (HIPAA), (Public Law 104-191): Requires health plans to assure the security and privacy of individually identifiable health information, and to use specified standards and code sets for electronic transactions involving medical information.
3. Coast Guard policy concerning the privacy rights of individuals and the Coast Guard's responsibilities for compliance with operational requirements established by The Coast Guard Freedom of Information and Privacy Acts Manual, COMDTINST M5260.3, and HIPAA are as follows:
- a. Privacy.
 - (1) Protect, as required by the Privacy Act of 1974, as amended, and HIPAA, the privacy of individuals from unwarranted intrusion. Individuals covered by this protection are living citizens of the United States and aliens lawfully admitted for permanent residence.
 - (2) Collect only the personal information about an individual that is legally authorized and necessary to support Coast Guard operations. Disclose this information only as authorized by the Privacy Act and HIPAA, and described in Chapter 4 of this Manual.
 - (3) Keep only personal information that is timely, accurate, complete, and relevant to the purpose for which it was collected.
 - (4) Safeguard personal information to prevent unauthorized use, access, disclosure, alteration, or destruction.
 - (5) Let individuals know what records the Coast Guard keeps on them and let them review or get copies of these records, subject to exemptions authorized by law.
 - (6) Permit individuals to amend records about themselves contained in Coast Guard systems of records, as authorized by HIPAA, which they can prove are factually in error, not up-to-date, not complete, or not relevant.
 - (7) Allow individuals to ask for an administrative review of decisions that deny them access to or the right to amend their records.
 - (8) Maintain only information about an individual that is relevant and necessary for Coast Guard purposes, as required to be accomplished by statute or Executive Order.
 - (9) Act on all requests promptly, accurately, and fairly.
 - b. Security.
 - (1) Facility Access Controls:

- (a) The Coast Guard will continually assess potential risks and vulnerabilities to individual protected health information in its possession, and develop, implement and maintain appropriate administrative, physical and technical security measures in accordance with HIPAA.
- (b) Clearly define the security perimeter of the premises and building. Ensure that the perimeter is physically sound. Ensure all external doors are adequately secured against unauthorized access by installing locks, alarms or other access control devices.
- (c) Define the instances in which visitors are allowed, including the areas they may visit and any escort requirements.
- (d) Ensure all doors to interior areas requiring compartmentalization or added security are adequately protected against unauthorized access by installing locks, alarms, or other access control devices.
- (2) Workstation Use and Security
 - (a) Comply with all applicable Coast Guard information system security policies.
 - (b) Log off every time prior to leaving the terminal
 - (c) Inspect the last logon information for consistency with actual last logon; report any discrepancies.
 - (d) Comply with all applicable password policies and procedures, including not storing written passwords.
 - (e) Close files and systems not in immediate use.
 - (f) Perform memory-clearing functions to comply with security policies.
- (3) Workforce Security
 - (a) Identify the extent of authorization each workforce member will require when accessing electronic protected health information, considering the criticality and sensitivity of the information to be handled.
 - (b) Workforce member, contractors and others shall access only those areas and the applicable health information to which they are authorized.
- (4) Information Systems Activity Review

- (a) Assign personnel to conduct a regular review of electronic protected health information systems' activities.
- (b) Reviewers should have appropriate technical skills to access and interpret audit logs correctly.
- (5) Contingency Plan
 - (a) Identify the hardware, software, applications and information sets that receive, manipulate, store and/or transmit electronic protected health information. Define information sets for the purpose of criticality rating.
 - (b) Identify backup methods and materials to be used, and the frequency of performing backups
 - (c) Monitor storage and removal of backups and ensure all applicable access controls are enforced.

4. Applicability and Scope.

- a. All health care facilities (clinics, super sickbays, and sickbays) shall comply with the MIS operating guidelines as set forth. The MIS program described here contains the essential elements required at all Coast Guard facilities with medical personnel assigned and assigns responsibilities for the program's initiatives. The Chief of Health Services shall ensure all healthcare providers and support staff; which include Medical Officers, Dental Officers, Pharmacy Officers, Clinic Administrators, HS's; HSD's and Medical and Dental contractors; shall participate. Information technology is not static in nature but rapidly changing and dynamic, and requires the diligence of all concerned to create and maintain a sound program.

5. Objectives.

- a. The Director of Health and Safety has established a MIS that provides necessary tools and capabilities to assist in making sound business decisions for those Commands having healthcare facilities.
- b. Identify and justify resources required to maintain a quality MIS.
- c. Establish access and connectivity for Coast-Guard wide comprehensive utilization of CHCS, continuing local DoD host site affiliation for electronic referrals and consultations.
- d. Establish and maintain clinic and sickbay Microcomputer Allowance Lists (MAL) that provide appropriate access to medical information systems for managing clinical and administrative operations.

- e. Establish a standardized equipment list for peripherals. (i.e. pharmacy printers, Local Area Network Interface Unit (LIU) devices, etc.)
 - f. Identify systems training requirements and ensure required education and training standards are established and maintained.
 - g. Provide direction as new adjuncts to existing programs are developed and deployed. (i.e. CHCS II, Theatre Medical Information Program (TMIP), etc.)
 - h. Participate in DoD sponsored software and product development for use in the medical arena.
6. Definitions.
- a. Intranet: A privately owned network based on the Transmission Control Protocol/Internet Protocol (TCP/IP) suite.
 - b. Internet: A voluntary interconnected global network of computers based upon the TCP/IP protocol suite, originally developed by the U.S. Department of Defense Advanced Research Projects Agency.
 - c. NIPERNET: Non-Classified Internet Protocol Routing Network. The Defense Information Systems network (DISN) Internet line for unclassified DoD and federal agency Internet traffic.
 - d. CGDN+: Coast Guard Data Network Plus. Secure closed Coast Guard wide area network (WAN).
 - e. Firewall: Security measure which blocks unwanted/unauthorized entry to computer systems from outside the internal system.
 - f. Host (site): Medical facility where a CHCS server platform resides.
 - g. TelNet: Telecommunications Network. A protocol that facilitates remote logins to host site server and functions via the Internet.
 - h. IP address: Internet Provider address. An assignable 32 bit numeric identifier, which designates a device's location on an intranet network or on the Internet.
 - i. LIU: Local Area Network Interface Unit. Device designed to provide external access and interface with the local area network (LAN).
7. Organizational Responsibilities.
- a. Chief, Office of Health Services.
 - (1) Establish a comprehensive MIS using the DoD Composite Health Care System (CHCS) and Dental Common Access System (DENCAS) at all Coast Guard health care facilities ashore and afloat.

- (2) Establish and promulgate MIS policy, including performance standards for use of all systems/applications contained within the program.
 - (3) Develop and promulgate MIS operation guidance detailing the various functional/operational requirements and adjuncts of the MIS program.
 - (4) Identify education and training requirements, and ensure satisfactory standards are established.
 - (5) Establish and maintain a Third Party Collection system for the recovery of reimbursable medical costs through Other Health Insurance (OHI).
- b. Maintenance and Logistics Commands.
- (1) Ensure the Health and Safety Directorate's MIS is executed at the field level.
 - (2) Provide technical and professional advice regarding medical information systems, software, and hardware to units as required.
 - (3) Coordinate professional training for MIS and health services personnel.
- c. Commanding Officers.
- (1) Ensure the unit actively pursues implementation and compliance with the health service MIS standards.
- d. Chief, Health Services Division.
- (1) Designate in writing an individual to serve as Health Services MIS Unit Site Manager for the Health and Safety Directorate's MIS.
 - (2) Implement and adhere locally to the Health and Safety Directorate's MIS policy.
 - (3) Ensure all health care facility personnel as prescribed, are in compliance of all provisions contained in this chapter.
- e. MIS Unit Site Manager.
- (1) Provide local level oversight of the Health and Safety Directorate's MIS.
 - (2) Coordinate and provide MIS training to health care facility staff.
 - (3) Coordinate and provide local systems hardware and software support.
 - (4) Coordinate with the cognizant Maintenance and Logistics Command (MLC) regarding hardware/software support issues beyond their ability to resolve.
 - (5) Establish liaison with medical appointment referral DoD Medical Treatment Facility (MTF) for MIS issues.

Section B - Medical Information System.

1. Background.

- a. Information technology is not static in nature but dynamic and rapidly changing. Commandant (G-WKH) is responsible for ensuring that the Health and Safety Directorate's MIS continues to evolve. The MIS has evolved from manual data collection systems of old, such as the old Daily Dental Workload sheets, to the Clinic Automated Management System (CLAMS) in the early 1990's. The late 1980's brought the DoD deployment of a hospital-based medical information system, the Composite Health Care System (CHCS). Concurrently, as the old Convergent Technology Operating System (CTOS) was phased out of the Coast Guard in the mid 1990's, CLAMS II was developed internally and deployed to Coast Guard clinics. The advent of TRICARE in the mid 1990's has necessitated integration of Coast Guard health care information with that of DoD's medical information infrastructure.

2. Systems. The following outlines current automated information systems, applications and program components that come under the Coast Guard MIS program.

a. Composite Health Care System (CHCS) I & II.

- (1) CHCS is the primary clinic/hospital based automated medical information system for DoD and is the legacy system, which will eventually transition to CHCS II. Major DoD commands generally act as host sites within their AOR. A "host" site is where the CHCS servers and database reside. Access to the functionality and modules of CHCS are accomplished through several options such as a closed internal network, through web based applications (i.e. Persona) or TelNet protocols. With the deployment of CHCS II, over 40 legacy and migration systems will integrate into a seamless clinical information system which will support readiness of forces, provide clinical data to enable health care providers to deliver quality managed care, and capitalize on technological advances to make a computer-based patient record (CPR) a reality. CHCS II will be the primary automated information system supporting the clinical business area within the DoD Health Affairs program.
- (2) Definitions.
 - (a) **Modules:** Particular functional features of the CHCS system.
 - (b) **Keys:** Security access tokens allowing access to modules within CHCS programs.
- (3) Modules.

- (a) **PHR:** Pharmacy. This module is used to input and process inpatient and outpatient medication orders and prescriptions. It is also used to maintain and record formulary files, bulk and clinic issues.
- (b) **MCP:** Managed Care Program. This module is used to perform patient enrollment, manage appointment referrals, perform provider searches, and to create and book appointments for enrolled and non-enrolled patients.
- (c) **ORE:** Order Entry. This module allows providers to enter orders that are immediately transmitted to other health care workers for implementation. Providers can create, modify sign, or counter-sign orders. Additionally, order information for individual patients can be retrieved for review.
- (d) **ERT:** Electronic Referral Tracking. This module allows providers to track the status and progress of patient referrals
- (e) **LAB:** Laboratory. This module allows health care professions to enter lab test orders, access test status, access test results, receive notification of problems running a test, and track patient test history.
- (f) **RAD:** Radiology. This module allows users to enter or modify radiological orders, view order status, and review the radiological impression.
- (g) **ADM:** Ambulatory Data Module. This module is used to track provider workload statistics, patient disposition, and patient diagnosis and procedure history.

b. SNAP Automated Medical System (SAMS).

- (1) The U.S. Navy's primary shipboard and sickbay medical information system program is SAMS. This application provides a user-friendly product that allows the Independent Duty Technician (IDT) to document all facets of health care; including patient encounters, medical and dental tickler system, and immunization tracking. SAMS functionality also offers users tools to produce binnacle lists, document shipboard training, and monitor environmental health issues such as heat stress and potable water testing. The fully functional tickler system flags crewmembers in need or past due for items such as physical examinations and immunizations, greatly enhancing operational readiness. Currently, SAMS is in the deployment planning stages.

(2) Definitions.

- (a) Modules: Particular functional features of the SAMS system.
- (b) AMMAL: Authorized Minimum Medical Allowance Level. This is analogous to the medical portion of the Health Services Allowance List.
- (c) AMDAL: Authorized Minimum Dental Allowance Level. This is analogous to the dental portion of the Health Services Allowance List.

(3) Modules.

- (a) Master Tickler: This module is used to document, update, report and transfer medical information on a crewmember. This module tracks demographic, physical examinations (routine, occupational and special duty), women's health maintenance examinations, allergies, immunization tracking, vision, hearing, dental readiness tracking, laboratory results, and sexually transmitted diseases.
- (b) **Medical Encounters:** This module is used to document and report health care encounters with the medical department. Specific encounters include routine sick call using the SOAP format, vital sign monitoring/tracking, follow-up examinations/visits, consultations and referrals, patient disposition accident and injury reporting.
- (c) **Occupational/Environmental Health:** This module documents environmental conditions that may affect the health of Coast Guard personnel. This module includes heat stress monitoring, potable water testing, and pest control.
- (d) **Supply Management:** This module supports the inventory management of medical material and pharmaceuticals. Support is provided for AMMAL and AMDAL inventory management. Users can requisition, store, distribute, and track all medical materials. The module produces a variety of inventory reports and maintains the Operating Target (OPTAR) log. The Coast Guard version of SAMS will utilize the Health Services Allowance List.
- (e) **Training Management:** This module tracks both crew and medical department personnel training. The module can be customized by the user to suit the needs of the unit.

- (f) **Periodic Duties:** This module provides supervisory personnel with a method to schedule, assign and track the completion of assigned tasks.
 - (g) **System Management:** This module maintains unit specific information, user table maintenance, and system utilities.
- c. Dental Common Access System (DENCAS).
 - (1) The Dental Common Access System is an enterprise-wide, world class e-business system that functions seamlessly between ship and shore to provide a complete picture of Navy and Coast Guard personnel dental readiness. DENCAS also provides an accurate, real-time, comprehensive administrative reporting system. The dental data is centralized in a single database for query by authorized staff over the NIPRNET. The DENCAS system is designed with security features that prevent unauthorized access, data transmission interception, and alteration. Navy Dental Treatment Facilities (DTF) and Coast Guard dental clinics are able to access dental data on individual active duty members from either service. However, summary dental data for each clinic is only available to their respective commands.
 - (2) Commanding officers are directed to ensure that Active Duty and Selected Reserve (SELRES) members assigned to their units comply with the medical/dental requirements of Chapter 3 of this manual. In an attempt to gain a more accurate assessment of dental readiness, commanding officers shall ensure that every member assigned to their unit have documented in DENCAS all dental exams and a current Dental Class status.
 - (3) Definitions.
 - (a) Modules: Particular functional features of the DENCAS system.
 - (b) DMD – Dental Management Data. These are the dental procedure codes representing provider productivity.
 - (c) NMIMC: Naval Medical Information Management Center. Responsible for DENCAS application support.
 - (4) DENCAS Access Levels.
 - (a) DTF User: This access level allows users to maintain patient dental and demographic information. It automatically updates Dental Class status, recall appointment intervals, documents dental treatment needs, allows for the transfer of patient dental data, tracks dental provider information, and records DMD (dental productivity) data. Additionally, this module can generate a variety of dental reports.

- 1 DTF User access should be granted to dental clinic staff members and Independent Duty Corpsmen. DTF Users must enter DENCAS data in a timely manner in order to ensure accurate dental readiness reports and patient information.
 - 2 Results from dental examinations completed by civilian, Army, and Air Force providers should be recorded on the SF 603 and DD Form 2813. The original DD Form 2813 should be maintained in the member's dental record. Units without an assigned Independent Duty Corpsman should send a copy of the DD Form 2813 to their respective MLC(k) to be transcribed into DENCAS.
- (b) DTF Admin User – This access level provides the same functionality as the DTF user. In addition, DTF Admin Users may issue and revoke DTF User certificates from personnel within their areas of responsibility (AOR).
 - (c) Command User: Command User functions are designed for use by the Maintenance and Logistics Commands (MLC) to review dental information on active duty members within their respective geographic AOR. This module displays the current dental readiness and dental health statistics for each command within their AOR. Command Users have access to the reports concerning individual patient dental class, recall appointments, and treatment needs. In addition, DMD data for each provider and dental clinic is available.
 - (d) Corporate User: This access level provides patient and DMD reports for all Coast Guard active duty members and Coast Guard dental clinics to the Coast Guard Headquarters Office of Health Services.
 - (e) External User: This module provides access to a number of useful reports on the real-time status of dental health within the External User's own command. When an External User first logs on to DENCAS, the Home Page displays the current status of dental readiness and dental health for the External User's own customer command. With a click on any of the report links on the page, the External User can view reports summarizing dental class, exam recall, members requiring routine dental care, and members requiring urgent dental care. Local commands (external customers) can obtain access to this level by contacting their respective MLC(k) or G-WKH-3. DTF Admin Users may also grant access.

- (f) System Management: This access level provides for system setup, table maintenance, and maintains system-related information such as user access, password configuration, and the access log. Responsibility for this module is shared between NMIMC and the Coast Guard Office of Health Services.
- (5) Modules.
- (a) Patient Information: DENCAS is designed to only track Coast Guard active duty and selected reserve (SELRES) members. The following guidance should be followed in order to facilitate accurate and consistent data entry and reports in DENCAS:
 - 1 Patient information (i.e., dental class, treatment needs, and exam date) should be recorded in DENCAS for only Coast Guard active duty and SELRES members. Entering patient information for dependents, retirees, and Department of Defense service members will result in errors in the dental readiness and exam compliance reports.
 - 2 DENCAS classifies patients as either “deployed” or “non-deployed”. Active duty members are classified as “deployed” and SELRES members as “non-deployed”. The Coast Guard uses this classification to separate active duty member patient information data from SELRES member data.
 - 3 Dental Class IV will be used to record that active duty and SELRES members do not have a dental exam on file in DENCAS or they are overdue for a dental exam.
 - 4 Patients with treatment needs marked as “urgent” should be classified as Dental Class III.
 - 5 Use of the “patient transfer” function should be kept to a minimum. All patient transfers will be done automatically by means of a monthly DEERS data import by the DENCAS system administrator.
 - (b) Provider: Provider productivity data should be entered under Dental Management Data (DMD) module for all categories of patients. Current Dental Terminology (CDT) codes are used to record all procedures.
 - 1 Dental procedure code “A9999” should be used to record each patient visit.
 - 2 A Daily Dental Procedures log sheet should be maintained for each provider to record on paper all completed dental

procedures. This log sheet is available as CG-6019, Daily Dental Procedures form on the Commandant (G-WK) website. Completed log sheets should be kept on file in the dental clinic for three years.

d. Third Party Collections Program: Other Health Insurance (OHI).

- (1) The United States Coast Guard is required by law to collect money from all third party insurance payers for the cost of medical services provided to military beneficiaries. This requirement, under Title 10 of the United States Code, Section 1095 is known as the Third Party Collection Program (TPC).
- (2) This program applies to family members and retirees who have health insurance coverage other than TRICARE, Medicare or Medicaid. Commanding Officers and Chiefs of Health Services will ensure that clinic staffs market the program and educate eligible beneficiaries based on guidelines provided by Commandant (G-WKH) program manager.
- (3) Each CG clinic will follow guidelines established by the Office of Health Services for documenting in CHCS any Other Health Insurance information non-active beneficiaries may have and facilitate the recovery of health care costs by adhering to guidelines provided by Commandant (G-WKH) program manager.

e. Protected Health Information Management Tool (PHIMT).

- (1) The Privacy Rule of the Health Information Portability and Accountability Act (HIPAA) requires a covered entity (i.e., the CG Health Care Program) to maintain a history of when and to whom disclosures of Protected Health Information (PHI) are made for purposes other than for treatment, payment and health care operations. The covered entity must be able to provide an accounting of these disclosures to an individual upon their request. Authorizations and Restrictions to disclosures from and individual to a covered entity are included in the information that is required for accounting purposes. Disclosures that are permitted but also must be accounted for are those made within six years of the date of request, in the following 12 categories:
 - (a) As required by law, statute, regulation or court orders,
 - (b) For public health reports, communicable disease control, FDA reports, and OSHA reports,

- (c) To government authorities regarding victims of abuse or domestic violence,
 - (d) To health oversight agencies,
 - (e) To judicial or administrative proceedings through an order from a court or administrative tribunal (or a subpoena if notice to the individual is provided),
 - (f) As required by law or court order, to identify a suspect, or to alert law enforcement of a crime,
 - (g) To funeral directors, coroners or medical examiners as authorized by law,
 - (h) To facilitate organ, eye or tissue donation,
 - (i) For research, as approved by a Review Board,
 - (j) To prevent a serious threat to health or safety,
 - (k) For execution of the military mission and other essential government functions, and
 - (l) To comply with workers' compensation laws.
- (2) To comply with the requirements for accounting for disclosures, the TMA has developed and provided an electronic disclosure tracking tool. The Protected Health Information Management Tool (PHIMT) stores information about Disclosures, Authorizations and Restrictions that are made for a particular patient. The PHIMT also has a functionality that can provide an accounting of disclosures by individual patient, upon request.
- (3) Use of the PHIMT is password protected, and several user roles are defined:
- (a) A regular user can create Disclosures and Authorization/Restriction requests.
 - (b) A user administrator can add/modify users within their Service.
 - (c) A Privacy/Security Officer can approve/deny Disclosures, Authorizations and Restrictions, and generate the associated letters.
- (4) A User Guide and an Administrator Guide for the PHIMT can be accessed through the HIPAA Learning Management Tool at www.HIPAAtraining.tricare.osd.mil using the student ID and password used for the HIPAA Privacy training modules.

Section C - Medical Readiness System (MRS).

1. The Medical Readiness System (MRS) is the Coast Guard's implementation of a modified off-the-shelf software application based on PeopleSoft's Human Resource Management System. It is primarily designed for use by clinics, independent duty health services technicians and Coast Guard Personnel Command (CGPC). MRS contains the following functional elements:
 - a. Recording Immunization Data
 - b. Physical Exam Currency
 - c. Medical Readiness Data
 - d. Color Vision Status
 - e. Waiver information
2. MRS is designed to enter and track medical readiness parameters (e.g. HIV test, PPD test, DNA specimen submission, physical exam currency, immunizations, color vision status, and medical waiver information) that assess operational readiness and are used extensively in other human resource programs.
3. MRS will also record waiver information. At the time a waiver is approved by CGPC, the cognizant division (opm-1, opm-2, rpm, epm-1) is responsible for entering medical waiver information into the appropriate MRS tables. This process began on 1 August 2002.
4. Questions on policy related to MRS implementation may be directed to COMDT (G-WKH).
5. Access Instructions:
 - a. To access the Medical Readiness System (MRS) you must be an authorized PeopleSoft user. Members will receive access to MRS after faxing a completed psc-7421/2 to (785) 339-3772. On the psc-7421/2, select "CGMRS - Medical Readiness System Clinical Access (Med care providers)" in block 7 for medical personnel or "CGMRSWVR – Medical Readiness Sys. Waiver Detail (Personnel Users)" for CGPC personnel. This form is located at the Personal Service Center (PSC) home page at: http://www.uscg.mil/hq/psc/forms/psc7421_2.pdf.
 - b. Access to the full MRS application is limited to medical and dental care providers (officer and enlisted) and staff members of COMDT (G-WKH), MLCLANT (k) and MLCPAC (k).
 - c. Access to the MRS Waiver Detail pages is limited to CGPC (opm-1, opm-2, rpm, epm-1).

- d. All users must complete a User Access Form (Appendix a) and submit their request to PSC Customer Care in order to receive a log on user name/password.
- (1) Complete Items 1 through 6 of the access form.
 - (2) Choose "CGMRS - Medical Readiness System Clinical Access (Med care providers)" in block 7 for medical personnel or "CGMRSWVR – Medical Readiness Sys. Waiver Detail (Personnel Users)" for CGPC personnel.
 - (3) Print the form
 - (4) User must sign and date item 10.
 - (5) Have the Unit CO, XO or Senior Medial Officer authority sign and date item 8 (forms signed "By direction" will not be accepted by PSC).
 - (6) Fax completed form to PSC Customer Care at 785-339-3772.